Cambridge OCR-set Assignment

Sample Assessment Material

Cambridge OCR Level 3 Alternative Academic Qualification
Cambridge Advanced Nationals in Cyber Security

Cambridge OCR Level 3 Alternative Academic Qualification
Cambridge Advanced Nationals in Cyber Security and Networks

Unit F195: Preventing cyberattacks

Scenario Title: Progress Health Services (PHS)

Valid for assessment until 20XX to 20XX.
For use by students beginning the qualification in September 20XX.

This is a sample Cambridge OCR-set assignment which should only be used for practice.

This assignment **must not** be used for live assessment of students.

The live assignments will be available on our secure website, 'Teach Cambridge'.

The Cambridge OCR administrative codes linked to this unit are:

- unit entry code F195
- certification code H037/H137

The regulated qualification numbers linked to this unit are:

610/6207/8 610/6208/X

Duration

About 15 hours of supervised time (GLH)

SAMPLE

© Cambridge OCR 2025

(work that **must** be completed under teacher supervised conditions)

All this material **can** be photocopied. Any photocopying will be done under the terms of the Copyright Designs and Patents Act 1988 solely for the purposes of assessment.

Contents

Information and instructions for teachers....3
Using this assignment....3
Information for delivering tasks....4
Tasks for students and assessment criteria....5
Scenario....5
Task 1....8
Task 2....10
Task 3....12
Task 4....14
NEA Command Words....16

© Cambridge OCR 2025

Information and instructions for teachers

Using this assignment

This assignment provides a scenario and set of related tasks that reflect how people working in cyber security will develop policies and procedures relating to information security and access.

You can give this to students on or after 1 June 202X to help them understand it before they start using it for assessment. The dates for which students can use it for assessment are shown on the front cover.

The assignment:
- Is written so that students have the opportunity to meet the requirements of all assessment criteria for the unit.
- Will tell students if their evidence must be in a specific format. If the task does not specify a format, students can choose the format to use.
- **Must** be completed under teacher supervision.

We have estimated that this assignment will take about 15 hours of supervised time to complete. Students should need approximately:
- 3 hours to complete Task 1.
- 3 hours to complete Task 2.
- 5 hours to complete Task 3.
- 4 hours to complete Task 4.

You **must**:
- Use a Cambridge OCR-set assignment for summative assessment of students.
- Familiarise yourself with the assessment criteria and assessment guidance for the tasks. These are given at the end of each student task. They are also with the unit content in **Section 5** of the Specification.
  Assessment guidance is only given where additional information is needed. There might not be assessment guidance for each criterion.
- Make sure students understand that the assessment criteria and assessment guidance tell them in detail what to do in each task.
- Read and understand **all** the rules and guidance in **Section 7** of the Specification **before** your students start the set assignments.
- Make sure that your students complete the tasks and that you assess the tasks fully in line with the rules and guidance in **Section 7** of the Specification.
- Give your students the **Cyber Security and Networks Student guide to NEA assignments before** they start the assignments.

You **must not**:

© Cambridge OCR 2025

- Use live Cambridge OCR-set assignments for practice or formative assessment. This sample assessment material **can** be used for practice or formative assessment.
- Use this sample assessment material for live assessment of students.
- Allow group work for **any** task in this assignment.
- Change any part of the Cambridge OCR-set assignments or assessment criteria.

Information for delivering tasks

Task	Requirements
Task 3	In Task 3 there is no requirement for students to implement any of the policies they design, however if centres have facilities to do this, students **could** demonstrate their policies as part of their evidence.

Pages 1-4 are for teachers only. Please do **not** give **Pages 1-4** to your students.

You can give **any** or **all** of the pages **that follow** to your students.

© Cambridge OCR 2025

Tasks for students and assessment criteria

Unit F195: Preventing cyberattacks

Scenario title: Progress Health Services (PHS)

Valid for assessment from September 20XX to 20XX.
For use by students beginning the qualification in September 20XX.

Scenario

PHS delivers bespoke training courses aimed at health in the workplace. The training courses can be delivered either onsite at PHS or at the offices of the business or school who have requested the training course. Awareness of mental health in the workplace and how employers should support this has increased throughout the country in recent years. This has led to a higher number of requests for PHS to deliver training. As a result, management at PHS have been discussing the possibility of creating online courses as well as their existing face-to-face courses.

PHS management is also aware of some of the cyber threats which have been widely reported in the news. They have been informed of the National Cyber Security Centre certification in Cyber Essentials, which can be used to assure customers that they have met a specific level of cyber security resilience. You have been hired by PHS who are considering applying for the Cyber Essentials certification.

Before applying for the Cyber Essentials certification, they have asked you to help them be better prepared for the certification process. You will need carry out an audit of their current cyber security practices and create cyber security policies and procedures to be implemented.

PHS have 15 members of staff who have a flexible working from home (WFH) policy, meaning they only have to go into the office when needed, for example for face-to-face meetings. There is a Local Area Network (LAN) which was developed when PHS first installed the network in 2010. The LAN is made up of a router, switch, and a Wireless Access Point (WAP). Data is stored onsite on the dedicated servers and users are authenticated by the domain server.

Staff are made up of:

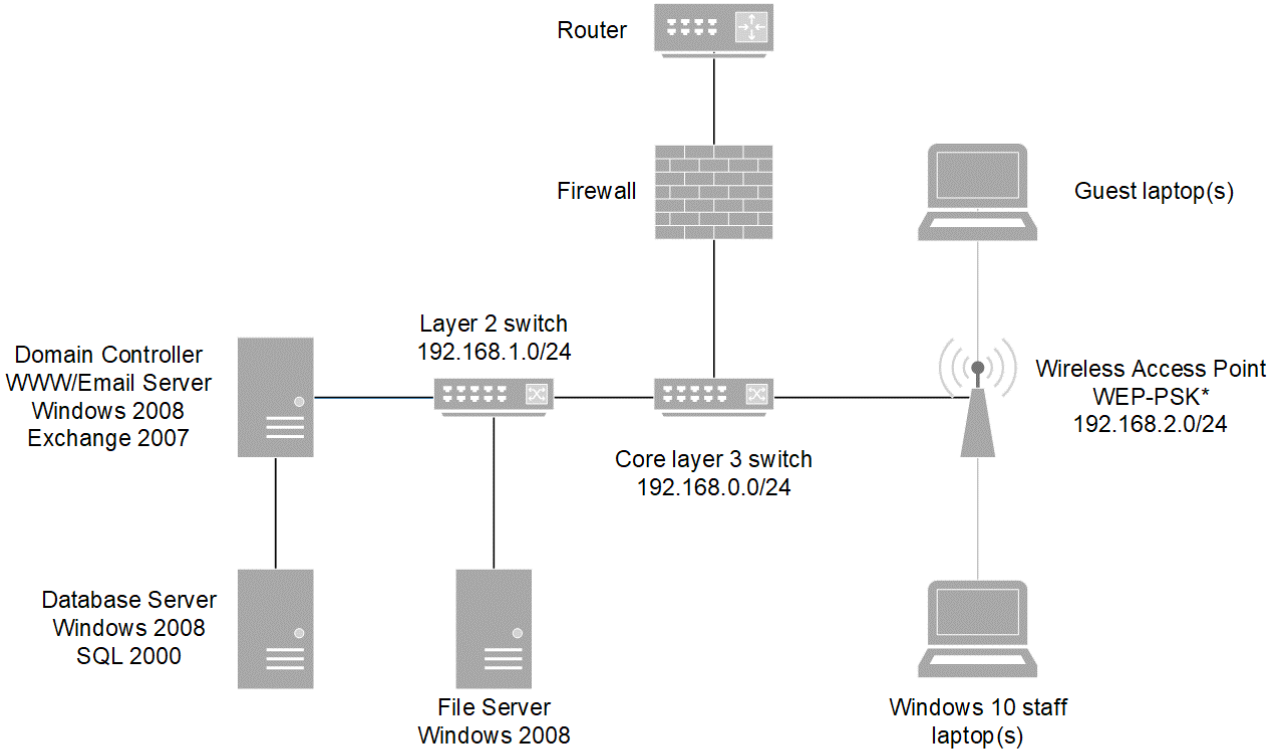
- The General Manager
- The Assistant Manager
- 10 Training staff
- 1 Human Resources Officer
- 1 Finance Officer
- 1 Part-time Safeguarding Officer.

Each member of staff has a laptop which they use both in the office and at home. The laptops were purchased in 2020 and have Windows 10 Pro installed with

© Cambridge OCR 2025

Microsoft Defender Antivirus for protection. The users are responsible for updating their laptops. There is no Extranet set up at present. If users need data or files to work on remotely, they either need to get the files before leaving the office or ask for the file to be shared/emailed by other members of staff.

This image shows the topology of the office network:



* Wired Equivelent Protection - Pre-Shared Key

The network was installed in 2010 and has not changed other than the implementation of the Windows 10 devices. The IT service company who installed the network and systems has since closed. The General Manager of PHS, who has no IT background, has taken responsibility of the server's upkeep, reaching out for support on forums when needing more experienced support. The configuration of the network is one core layer 3 switch which manages Virtual LANs (VLANs), a Layer-2 switch for the servers, and a Wireless Access Point (WAP) which allows wireless devices to access the internet and the services on the LAN.

Each physical server is configured to host specified services, but their software and firmware versions are the same as the day they were installed. Accounts are created and managed on the Domain Controller, but these are set to access emails. There is currently no access control on the Database and File Servers from within the LAN. The Firewall is configured to forward outside traffic to the World Wide Web (WWW) Server using both HTTP and HTTPS, but all internal traffic is permitted to pass from internal devices to the internet.

Files used by all users are stored on the File Server. However, there have been occurrences where multiple copies of files have existed. This is often due to individual staff members needing access to files or information at once or when

© Cambridge OCR 2025

working remotely. Some files have been encrypted using a password to secure some sensitive information, but the same password is used for all files.

Progress Health Services' (PHS) Laptop, Email and Internet Use Policy.

1. Users must use laptops for work purposes only.
2. Users must only access work files using their work laptop and not on a personal device. Any files taken off site must be password encrypted.
3. Users must not use bad language in any email they send or attempt to bully or harass anyone.
4. Users must not visit sites which might have material which others might find offensive – pornography, racist, violent or similar sites.
5. Users must not share company data with third parties.
6. Users must make sure that work laptops are updated.
7. Users must scan any downloaded files for viruses.
8. Users must not use any laptop in such a way that would disrupt the laptop use of others, nor interfere with any security measures the company may have in place.
9. All passwords must be:
   - At least 8 characters
   - Must be a combination of upper case letters, lower case letters and numbers.

© Cambridge OCR 2025

Task 1
Creating a risk assessment

Topic Areas 1 and 2 are assessed in this task

The task is:

Create a risk assessment for the organisation.

- You will use appropriate tools and techniques to create the risk assessment for Progress Health Services (PHS) which identifies cyber security risks.
- You will also define the level of severity of each risk and identify the assumptions made.

Your evidence **must** include:

- A risk assessment.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td>P1: Create a risk assessment appropriate for the organisation.
(PO4)</td><td rowspan="2">M1: Explain how the risks identified could impact the network and data security of the organisation.
(PO2)</td><td rowspan="3">D1: Evaluate the tools and techniques used to identify risks and their level of severity.
(PO3)</td></tr>
<tr><td>P2: Use a risk matrix to define the severity level of each risk identified.
(PO4)</td></tr>
<tr><td>P3: Identify three assumptions made when defining the severity of the risks.
(PO2)</td><td>M2: Justify the assumptions identified when defining the severity of the risks.
(PO3)</td></tr>
</table>

© Cambridge OCR 2025

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P1	• Students **must** use appropriate tools and techniques to create their risk assessment. The risk assessment must cover **all** risks detailed in the scenario. • Students **must not** be given a template to complete this task.
P2	• Students **must** define the severity of all risks identified in P1. To define each risk's severity, students **could** use the risk matrix format from Topic Area 2.2 or another standard risk matrix format they have been taught.
P3	• There is no additional assessment guidance for this criterion.
M1	• Students **must** explain how the risks detailed in P1 and P2 could impact the organisation's network(s) and data security.
M2	• There is no additional assessment guidance for this criterion.
D1	• Students **must** include in their evaluations an assessment of the effectiveness of the tools and techniques they used to identify risks and their level of severity.

© Cambridge OCR 2025

Task 2
Auditing cyberattack prevention measures and recommending improvements

Topic Areas 1, 3, 4 and 5 are assessed in this task

The task is:

Audit the existing cyberattack prevention measures used by the organisation.

- You will audit the cyberattack prevention policies, procedures and methods used by Progress Health Services (PHS).
- You will need to identify the gaps found in the existing cyberattack policies, procedures and methods used.

Your evidence **must** include:

- An audit of the existing cyberattack prevention measures.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P4: Complete an audit of the existing cyberattack prevention measures used. (PO4)	**M3: Assess** the strengths and weaknesses of the existing cyberattack policies, procedures and methods identified in the audit. (PO3)	**D2: Discuss** how each improvement to the organisation's cyber security policies, procedures and methods will enhance their cyber security. (PO3)
P5: Identify the gaps in the existing cyberattack policies, procedures and methods used. (PO2)	**M4: Describe** improvements to each of the existing cyberattack policies, procedures and methods used. (PO2)	

© Cambridge OCR 2025

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P4	• Students **must** audit **all** the existing cyberattack policies, procedures and methods used by the organisation in the scenario.
P5	• Students **must** identity where the existing cyberattack policies, procedures and methods, used by the organisation in the scenario, do not sufficiently protect them from the risks identified in Task 1.
M3	• M3 builds on P4. For **each** cyberattack measure identified in the audit, students **must** assess how well it protects the organisation in the scenario from cyberattacks. Where weaknesses and/or any non-conformities (NCR) are found, students **must** include the impact these could have on the organisation's operations.
M4	• M4 builds on P5. Students **must** describe at least **one** specific improvements to each existing cyberattack policy, procedure and method used by the organisation in the scenario.
D2	• D2 builds on M3 and M4. Students **must** discuss how the recommended improvements will: o reduce the risk to the organisation's network data security and o improve the organisation's overall cyber security.

© Cambridge OCR 2025

Task 3
Designing cyber security prevention measures

Topic Areas 1, 3, 4 and 5 are assessed in this task

The task is:

Design cyber security prevention measures for the organisation.

- You will design access control policies and written user policies which improve the cyber security protection of Progress Health Services' (PHS) systems and users.

Your evidence **must** include:

- Access control policies.
- Written user policies.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P6: Design access control policies for external access to systems/networks. (PO4)	**M5: Design** cyber security prevention measures which make use of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). (PO4)	**D3: Justify** how each cyber security prevention policy and measure designed relate to the concepts of cyber security. (PO3)
P7: Design access control policies for internal access to systems/networks. (PO4)		
P8: Design access control policies for access rights of different user groups. (PO4)		
P9: Design written user policies which outline how technology should be used in the organisation. (PO4)		

© Cambridge OCR 2025

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P6 **P7** **P8** **M5**	• Students **must** choose appropriate methods and use them to design policies which will improve the organisation in the scenario's cyber security. Students **could** use content from Topic Areas 3 and 4. • Designs **must** include how the policies will be setup/configured and **could** include diagrams as well as written text. • There is no requirement for students to implement any of their policies, however if centres have facilities to do this, students **could** demonstrate their policies as part of their evidence.
P9	• Students **must** design written user policies which will indicate how users from the organisation should and shouldn't use the network. Topic Area 5 contains common written user policies and students only need to design those which are appropriate to/relevant for the organisation in the scenario.
D3	• Students **must** use the content in Topic Area 1.1 to help them discuss how well each of the cyber security prevention policies and measures designed relates to the concepts of cyber security.

© Cambridge OCR 2025

Task 4
Reviewing the designed cyber security prevention measures

Topic Areas 1, 2, 3, 4, 5 and 6 are assessed in this task.

The task is:

You will review the cyber security prevention measures designed for Progress Health Services (PHS) in **Task 3**.

Your evidence **must** include:

- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P10: Describe the purpose of each policy and measure designed. (PO2)	**M6: Explain** how each policy and measure designed could be implemented. (PO2)	**D4: Discuss** the impact of implementing each policy and measure designed on the users of the organisation's system. (PO3)
P11: Explain how each policy and measure designed prevents exposure to cyber security threats. (PO2)	**M7: Analyse** the advantages and disadvantages of each policy and measure designed. (PO3)	**D5: Evaluate** the effectiveness of each policy and measure designed in reducing the cyber security risks identified. (PO3)
P12: Explain how each policy and measure designed reduces the likelihood and severity of cyber security risk. (PO2)		

© Cambridge OCR 2025

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P10	• Students **must** describe the purpose of each policy and measure designed in Task 3.
P11	The focus of P11 and P12 is different. • P11 focuses on how each policy and measure designed in Task 3 aims to eliminate the exposure to cyber security threats that pose a potential loss. • P12 focuses on how each policy measure designed in Task 3 reduces the likelihood and severity of a possible loss from cyber security threats.
P12	
M6	• Students **must** explain how the organisation in the scenario would implement policies they designed in Task 3. The implementation explanations **must** be at a high level rather than a step-by-step guide. Students **must** also explain how they would "roll out" their written policies to staff.
M7	• There is no assessment guidance for this criterion.
D4	• D4 builds on M6. Students **must** discuss how users will be impacted by the implementation of the policies designed in Task 3. This **must** include how their "usage" may change and any negative impact they may experience.
D5	• Students **must** evaluate how well their policies and measures ensure that the more severe risks identified in Task 1 and insufficiencies/gaps in protection identified in Task 2 are mitigated. If any insufficiencies/gaps in protection remain, students **must** justify why these have not been addressed.

© Cambridge OCR 2025

NEA Command Words

The table below shows the command words that may be used in the NEA assignments and/or assessment criteria.

Command Word	Meaning
Adapt	• Change to make suitable for a new use or purpose
Analyse	• Separate or break down information into parts and identify their characteristics or elements • Explain the different elements of a topic or argument and make reasoned comments • Explain the impacts of actions using a logical chain of reasoning
Assess	• Offer a reasoned judgement of the standard or quality of situations or skills. The reasoned judgement is informed by relevant facts
Calculate	• Work out the numerical value. Show your working unless otherwise stated
Classify	• Arrange in categories according to shared qualities or characteristics
Compare	• Give an account of the similarities and differences between two or more items, situations or actions
Conclude	• Judge or decide something
Describe	• Give an account that includes the relevant characteristics, qualities or events
Discuss (how/whether/etc)	• Present, analyse and evaluate relevant points (for example, for/against an argument) to make a reasoned judgement
Evaluate	• Make a reasoned qualitative judgement considering different factors and using available knowledge/experience
Examine	• To look at, inspect, or scrutinise carefully, or in detail
Explain	• Give reasons for and/or causes of something • Make something clear by describing and/or giving information
Interpret	• Translate information into recognisable form • Convey one's understanding to others, e.g. in a performance
Investigate	• Inquire into (a situation or problem)
Justify	• Give valid reasons for offering an opinion or reaching a conclusion
Research	• Do detailed study in order to discover (new) information or reach a (new) understanding
Summarise	• Express the most important facts or ideas about something in a short and clear form

We might also use other command words but these will be:

© Cambridge OCR 2025

- commonly used words whose meaning will be made clear from the context in which they are used.
- subject specific words drawn from the unit content.

© Cambridge OCR 2025